# REMARKS

Claims 1-18 are pending in the application. Claim 5 was objected to for informalities, as described in paragraph 2 of the Office Action. Claims 1-18 were rejected under 35 U.S.C. § 103 (a), as described in paragraph 3 of the Office Action. Claims 1, 3, 7, 9, 13 and 15 are the only independent claims.

Item 12 of the Office Action Summary acknowledges a claim of foreign priority, but fails to clearly specify that a certified copy of the priority document has been received. Accordingly, Applicants request that the record clearly indicate that the certified document of the priority document has been received by the USPTO.

The specification has been amended to place the application in correct idiomatic English.

Claim 5 has been amended as suggested in paragraph 2 of the Office Action. Accordingly, it is respectfully requested that the outstanding rejection to claim be withdrawn.

The "means for" and "step of" language throughout claims 1-18 has been deleted so that claims 1-18 will not be construed under 35 U.S.C. § 112, sixth paragraph. The remainder of the amendments to claims 1-18 generally place the claims in better U.S. form without narrowing the scope of the claim as originally presented.

It is respectfully submitted that claims 1-18 are patentable over Nakamura et al. (Nakamura) in view of Barton, within the meaning of 35 U.S.C. § 103, for the following reasons.

In accordance with one aspect of the present invention is drawn to embedding tamper-detection-information, for example as illustrated in Fig. 1, wherein a pseudo-random number series is generated by using predetermined key data, and authentication data is generated from the pseudo-random number series. Further, the key data is embedded in transform coefficients of a lowest frequency band (i.e., MRA illustrated as LL3 in FIG. 6) among a plurality of frequency bands. Finally, authentication data is embedded in transform coefficients of the remaining frequency bands exclusive of the MRA ( i.e., MRR illustrated as all other components in FIG. 6) among the plurality of frequency bands.

Independent claim 1 is drawn to an apparatus of the above-identified aspect, whereas claim 7 is drawn to a method of performing the above-identified aspect, and whereas claim 13 is drawn to a recording medium having computer device readable instruction operable to instruct a computer device to perform the above-identified aspect.

Independent claim 1 requires, *inter alia*, an authentication data generation portion operable to "generate a pseudo-random number series by using predetermined key data, and to **generate authentication data from the pseudo-random number series**." Similarly, each of independent claims 7 and 13 require, *inter alia*, generating "a pseudo-random number series by using predetermined key data, and **generating authentication data from the pseudo-random number series**." Further, claim 1 requires a key data embedding portion operable to **embed the key data in transform coefficients of a lowest frequency band** among the plurality of frequency bands." Similarly, each of independent claims 7 and 13 require "**embedding the key data in transform coefficients of a lowest frequency band** among the plurality of frequency bands." Claim 1 additionally requires an authentication embedding portion operable to "**embed the authentication data in transform coefficients of the frequency bands exclusive of the MRA** among the plurality of frequency bands." Similarly, each of independent claims 7 and 13 require "**embedding the authentication data in transform coefficients of the frequency bands exclusive of the MRA** among the plurality of frequency bands."

Another aspect of the present invention is drawn to tamper detection, wherein key data that is embedded in transform coefficients of a lowest frequency band (i.e., the MRA) among the plurality of frequency bands is extracted. Further, a pseudo-random number series is generated using the key data, and authentication data is generated from the pseudo-random number series. Finally, embedded information is extracted, wherein the embedded information is embedded based on the key data from transform coefficients of the frequency bands exclusive of the MRA (i.e., the MRR) among the plurality of frequency bands.

Independent claim 3 is drawn to an apparatus of the above-identified aspect, whereas claim 9 is drawn to a method of performing the above-identified aspect, and whereas claim 15 is drawn to a recording medium having computer device readable instruction operable to instruct a computer device to perform the above-identified aspect.

Independent claim 3 requires, *inter alia*, a key data extraction porti on operable to "**extract key data** embedded by the specific apparatus **from transform coefficients of a lowest frequency band** among the plurality of frequency bands." Similarly, each of independent claims 9 and 15 require, *inter alia*, "**extracting key data** embedded by the specific apparatus **from transform coefficients of a lowest frequency band** among the plurality of frequency bands." Further, claim 3 requires an authentication data generation portion operable to "generate a pseudo-random number series by using the key data, and **to generate authentication data from the pseudo-random number series**." Similarly, each of independent claims 9 and 15 require "generating a pseudo-random number series by using the key data, and **generating authentication data from the pseudo-random number series**." Claim 3 additionally requires an embedded information extraction portion operable to "**extract embedded information** embedded based on the key data by the specific apparatus **from transform coefficients of the frequency bands exclusive of the MRA** among the plurality of frequency bands." Similarly, each of independent claims 9 and 15 require "**extracting embedded information** embedded based on the key data by the specific apparatus **from transform coefficients of the frequency bands exclusive of the MRA** among the plurality of frequency bands."

It is respectfully submitted that neither Nakamura nor Barton teaches the above-identified emphasized limitations.

Nakamura discloses an apparatus and a method for embedding digital watermark information in image data. In Nakamura, a random-number-generator 119 generates one random number 120 per bit of the digital watermark-information 104 to be embedded. The random-number-generator 119 generates a sufficiently large figure to prevent random number conflicts by using an initial-value-of-a-random-sequence 31. An information-embedding-section 121 selects one coefficient, to which a bit value is embedded, from amongst the M × N × T coefficient matrix based on the generated random number, and changes its value according to a bit value to be embedded. This process is performed for all bits of the digital watermark information, thereby embedding the digital watermark information in the image data.

Barton discloses an authentication technique by embedding arbitrary digital information within a stream of digital data and extracting the embedded information.

Page 4 of the Office Action indicates that Nakamura "does not explicitly teach generating authentication data from the pseudo-random number series." As each of claims 1-18 are rejected, it is presumed that this statement is a shorthand assertion that Nakamura fails to explicitly teach the authentication data generation portion, as required in either one of independent claims 1 and 3; or the generating, as required in either one of independent claims 7, 9, 13 and 15. Nevertheless, the Office Action therefore relies on Barton, for allegedly disclosing "a method and apparatus for generating an embedding authentication information of a digital block (Barton Fig. 2, column 4, lines 22-41 and column 7, line 55 - column line 28)."

While not commenting of the alleged teachings of Barton discussed on page 4 of the Office Action, it is respectfully submitted that Barton fails to teach or suggest that "**authentication data is generated from a pseudo-random series**." On the contrary, as discussed in column 4, lines 22-25, Barton merely teaches that the authentication information is "provided by the user."

Because neither Nakamura nor Barton teaches or suggest generating a pseudo-random number series by using predetermined key data and generating authentication data from the pseudo-random number series, it is respectfully submitted that a combination of the teachings of Nakamura and Barton additionally fails to teach such a feature.

In light of the above discussion, it is respectfully submitted that a combination of the teachings of Nakamura in view of Barton fails to teach: the authentication data generation portion, as required in either one of independent claims 1 and 3; or the generating, as required in either one of independent claims 7, 9, 13 and 15.

Page 5 of the Office Action indicates that Nakamura does not explicitly disclose "key data extraction means for extracting said key data embedded by said specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among said plurality of frequency bands." The Office Action therefore relies on Barton for allegedly disclosing "a method and apparatus for generating, embedding and extracting authentication information of a digital block (Barton Fig. 2, column 4, lines 22-41 and column 7, line 55 – column line 28)."

It is clear from the Office Action that the Examiner has failed to establish a *prima facie* case of obviousness within the meaning of 35 U.S.C. § 103. In particular, the Office Action admits that Nakamura does not disclose the required extraction means. However, the Office Action fails to provide other evidence, in the form of prior art references or sound scientific reasoning, of the shortcomings of Nakamura such that a combination of the teachings of Nakamura and the other evidence would teach that which is required in the claimed invention. Specifically, the Office Action relies on the teaching of Barton, but fails to assert (correctly in this case) that Barton teaches "key data extraction means for extracting said key data embedded by said specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among said plurality of said frequency bands."

Because neither one of Nakamura and Barton teaches or suggests "**key data extraction means for extracting said key data embedded by said specific apparatus from transform coefficients of a lowest frequency band among said plurality of said frequency bands**," it is respectfully submitted that a combination of the teachings of Nakamura and Barton additionally fail to teach such a feature.

In light of the above discussion, it is respectfully submitted that the Examiner has failed to establish a *prima facie* case of obviousness, and more importantly that a combination of the teachings of Nakamura in view of Barton fail to teach or suggest: a key data extraction portion, as required in independent claim 3; extracting key data, as required in independent claim 9; or extracting key data, as required in independent claim 15.

In view of the above remarks, Applicant respectfully submits that claims 1, 3, 7, 9, 13 and 15 would not have been obvious over the combination of Nakamura in view of Barton, and urge that the rejection of claims 1-18 under 35 U.S.C. § 103(a), be withdrawn.

Having fully and completely responded to the Office Action, Applicants submit that all of the claims are now in condition for allowance, an indication of which is respectfully solicited.

If there are any outstanding issues that might be resolved by an interview or an Examiner's amendment, the Examiner is requested to call Applicants' attorney at the telephone number shown below.

Respectfully submitted,

Hisashi INOUE et al.

By: Thomas D Robbins
Thomas D. Robbins
Registration No. 43,369
Attorney for Applicants

TDR/jlg
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
August 6, 2004

THE COMMISSIONER IS AUTHORIZED
TO CHARGE ANY DEFICIENCY IN THE
FEES FOR THIS PAPER TO DEPOSIT
ACCOUNT NO. 23-0975